Financial Cybercrime Task Force of Kentucky

Risk Advisory Bulletin

February 18, 2015 ***Bulletin Reference #B0218-03***

Subject: Microsoft Ending Support for Windows Server 2003 Operating System

Purpose: The DFI's Financial Cybercrime Task Force of Kentucky issues this Bulletin to the financial services industry in Kentucky related to risks associated with continuing to run Windows Server 2003 after July 14, 2015.

Background: On July 14, 2015, Microsoft is scheduled to end support for the Windows Server 2003 operating system. After this date, systems using this operating system will be at risk as this product will no longer receive:

- Security patches that help protect PCs from harmful viruses, spyware, and other malicious software,
- Assisted technical support from Microsoft, and
- Software and content updates.

Recommendations: Computers running the Windows Server 2003 operating system will continue to work after support ends. However, using unsupported software may increase the risks of viruses and other security threats. Negative consequences could include loss of confidentiality, integrity, and/or availability of data, system resources and business assets.

Users should consider:

1. Upgrading to a currently supported operating system or other cloud-based services. If needed, there are software vendors and service providers in the marketplace who offer assistance in migrating from Windows Server 2003 to a currently supported operating system or SaaS (software as a service) / IaaS (infrastructure as a service) products and services.

2. Verifying that third-party service providers have properly addressed the Windows Server 2003 concern. Management needs to determine that vendors with whom the institution shares customer non-public personal information have appropriately addressed this issue to prevent unauthorized access and loss of the information entrusted to them.

As always, ensure employees use caution when accepting information, data, or documents that were created or stored on an external computer, especially via a thumb drive or other storage device, and that proper online banking authentication is in place.

For more information, view the alert issued by US-CERT at https://www.us-cert.gov/ncas/alerts/TA14-310A.

If you have any questions regarding this Bulletin, please contact dfi.reporting@ky.gov.

The Financial Cybercrime Task Force of Kentucky is a proactive, internal work group of DFI that focuses on best practice guidance and warnings for the financial services industry. The Task Force's goal is to identify and address emerging threats in cybercrime and security and to protect the integrity of the Kentucky financial system.

DFI, http://kfi.ky.gov, is an agency in the Public Protection Cabinet. For more than 100 years it has supervised the financial services industry by examining, chartering, licensing and registering various financial institutions, securities firms and professionals operating in Kentucky. DFI's mission is to serve Kentucky residents and protect their financial interests by maintaining a stable financial industry, continuing effective and efficient regulatory oversight, promoting consumer confidence, and encouraging economic opportunities.